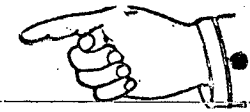
Organization TC 2600 Bldg./Room KNOX
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS



RETURN TO SENDER

NO SUCH #
ATTEMPTED - NOT KNOWN
VACANT
ROUTE NUMBER 2909
INITIALS

U.S. OFFICIAL MAIL
PENALTY FOR
PRIVATE USE $300
PITNEY BOWES
02 1A
0004204479
$ 01.06⁰
SEP 19 2005
MAILED FROM ZIP CODE 22314

AN EQUAL OPPORTUNITY EMPLOYER

RECEIVED
SEP 2 6 2005
USPTO MAIL CENTER

BEST AVAILABLE COPY

IFW -

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/875,261	06/05/2001	Todd F. Mozer	016757-000800US	4605

7590 09/19/2005

EXAMINER
LERNER, MARTIN

ART UNIT	PAPER NUMBER
2654	

DATE MAILED: 09/19/2005

Chad Walsh, Esq.
Fountainhead Law Group
6172 Bollinger Road, #174
San Jose, CA 95129

RECEIVED
OIPE/IAP

SEP 27 2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/875,261	MOZER, TODD F.	
	Examiner	Art Unit	
	Martin Lerner	2654	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 to 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 to 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1 to 6, 9 to 13, 18 to 19, 21 to 23, 25 to 27, 31, 35 to 36, and 38 to 42 are rejected under 35 U.S.C. 102(e) as being anticipated by *Ritter*.

Regarding independent claims 1, 9, and 31, *Ritter* discloses a method and system for authenticating persons, comprising:

"a client system receiving first and second biometric data from a user, the client system having a first level security authorization procedure, wherein the first level security authorization denies access to the client system if the first biometric data does not correspond to an authorized user" – authentication of a user through a communication terminal device ("a client system") can be used to allow or refuse a user the usage of the communication terminal in correspondence with the result of the authentication ("a first level security authorization procedure" "denies access to the client system"), where the result of the authentication at a mobile communication

terminal device can also be transmitted in a wireless manner (column 1, line 65 to column 2, line 6: Figure 1); a user can insert his personal SIM-card 3 in a communication terminal device 1; communication terminal 1 is equipped with a video sensor 2 for recording body features, such as eye patterns 6, facial features 7, or fingerprints 8 (column 4, lines 16 to 21: Figure 1); from this data, biometric keys are derived which are temporarily stored (column 4, lines 32 to 37: Figure 1); body features such as eye patterns, facial features, or fingerprints are "first biometric data from a user"; personal SIM-card 3 has stores tables 4 having biometric keys (column 3, line 57 to column 4, line 2: Figure 1); tables 4 of biometric keys stored on SIM-card 3 are "second biometric data from a user";

"a server system receiving the second biometric data from the client and having a second level security authorization procedure" – a result of authentication by a mobile communication terminal device can also be transmitted in a wireless manner to an external secured device, which, for its part, can permit or refuse access to its building or services (column 2, lines 2 to 6: Figure 1); in addition to a direct comparison at a mobile radio telephone 1, authenticity and integrity of the stored biometric keys 4 can be confirmed by means of trusted third party (TTP) services by a biometric server 10 (column 4, lines 38 to 52: Figure 1);

"wherein the first level security authorization procedure and the second level security authorization procedure comprise distinct biometric algorithms" – if the comparison of the current biometric key to the biometric key 4 stored in the SIM-card 3 turns out to be positive and if the stored biometric keys 4 are authenticated positively by

biometric server 10, further usage of the mobile radio telephone 1 may be granted (column 4, lines 38 to 52: Figure 1); thus, a first level security algorithm is performed at a client/terminal to compare biometric data of a user to biometric data on a user's card, and a second level security algorithm is performed at a server to compare biometric data of a user to biometric data of all valid users; further comparison prevents usage of fraudulent SIM-cards.

Regarding claims 2 to 4, *Ritter* discloses biometric data includes voice features (column 3, lines 7 to 10; column 4, line 31 to 35) and personal user profile passwords (column 3, lines 11 to 32).

Regarding claims 5, 6, 10, and 11, *Ritter* discloses a first level security algorithm is performed at a client/terminal to compare biometric data of a user to biometric data on a user's card, and a second level security algorithm is performed at a server to compare biometric data of a user to biometric data of all valid users (column 4, lines 38 to 52: Figure 1).

Regarding claim 12, *Ritter* discloses a server automatically executes authentication again after a predetermined period (column 4, lines 48 to 52: Figure 1).

Regarding claim 13, *Ritter* discloses that if comparison turns out to be positive, further usage of a mobile radio telephone may be permitted (column 4, lines 40 to 45: Figure 1); implicitly, permitting usage of a mobile radio telephone involves "receiving control information" from an authentication program on mobile radio telephone to enable usage.

Regarding claims 18 to 19, 21 to 23, and 35 to 36, *Ritter* discloses a personal user profile establishes levels of access rights to different services ("a plurality of server resources"; "a plurality of remote network resources"), and duration of validity to limit the validity of certain rights to specific duration of time or point in time (column 3, lines 17 to 32: Figure 1); permission to use a mobile radio terminal, via a mobile network, may be sustained for a limited time period ("allowable network connection time") (column 4, lines 47 to 52: Figure 1).

Regarding claims 25 to 27, *Ritter* discloses storing biometric keys on a server (column 3, lines 40 to 47); biometric data can be voice features ("a digital voice print") or fingerprints (column 3, lines 7 to 10; column 4, lines 16 to 32: Figure 1).

Regarding claims 38 to 41, *Ritter* discloses biometric data includes voice features (column 3, lines 7 to 10; column 4, line 31 to 35) and personal user profile passwords (column 3, lines 11 to 32); implicitly, authentication by voice features involves a speaker recognition algorithm.

Regarding claim 42, *Ritter* discloses storing biometric keys on a personal SIM-card (column 1, lines 46 to 53: Figure 1), which is a smart card.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 7, 8, 14 to 17, 24, and 32 to 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ritter* in view of *Su et al.*

Concerning claims 7 and 8, *Ritter* does not expressly disclose security authorizations with a neural network and Hidden Markov Models. However, it is well known that speech recognition and verification algorithms utilize neural networks and Hidden Markov Models as ways of performing speech recognition and verification. Specifically, *Su et al.* teaches creating speaker models by neural networks and Hidden Markov Models. (Column 6, Lines 1 to 10) It is would have been obvious to one having ordinary skill in the art to utilize neural networks and Hidden Markov Models as taught by *Su et al.* in the authentication method and system of *Ritter* because it is well known that these are the main algorithms for performing recognition and verification.

Concerning claims 14 to 17 and 32 to 34, *Ritter* does not disclose control information comprising a verification confidence value, modifying an acceptance threshold, and prompting the user for additional information if verification confidence is in a first range. However, *Su et al.* teaches a security application, where a user can select a desired level of security and threshold levels are adjusted to accommodate the particular level of security desired. (Column 8, Line 59 to Column 9, Line 7: Figure 4) Pattern matching produces a particular score ("verification confidence value") for comparison and deciding whether to accept or reject a speaker. (Column 7, Lines 8 to 23) A user is asked for more repetitions for higher levels of security. (Column 8, Line 36 to Column 9, Line 39) *Su et al.* states an advantage is maintaining a high level of security that alleviates the problem of requiring the user to memorize passwords.

(Column 1, Lines 29 to 47) It would have been obvious to one having ordinary skill in the art to modify a threshold level in a speaker verification system as suggested by *Su et al.* in the authentication method and system of *Ritter* for the purpose of alleviating the problem of requiring the user to memorize passwords.

Concerning claim 24, *Ritter* discloses text-prompted speaker verification (column 3, lines 59 to 67), which involves "an identification script to obtain identification information about the user".

5. Claims 20 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ritter* in view of *Gifford*.

Ritter discloses time limitations (column 3, lines 26 to 32; column 4, lines 48 to 53), but does not specifically provide authorization criteria of spending amount limitations. However, *Gifford* teaches an open network payment system, where authentication is provided for spending limits for any duration of time so as to limit fraud risk. (Column 8, Line 65 to Column 9, Line 18) It would have been obvious to one having ordinary skill in the art to provide for spending limits as suggested by *Gifford* in the authentication method and system of *Ritter* for the purpose of limiting risk of fraud.

6. Claims 28 to 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Ritter* in view of *Su et al.* as applied to claim 9 above, and further in view of *Maurer et al.*

Su et al. suggests background noise conditions affect speaker verification (column 6, lines 60 to 67), changing recognition algorithms by varying the script (column

8, lines 27 to 58), and changing recognition parameters by adjusting the threshold (column 8, line 59 to column 9, line 7). However, *Su et al.* omits changing recognition algorithms and recognition parameters based upon line quality measures. *Maurer et al.* teaches evaluating the quality of a transmission channel using voice recognition for the purpose of providing a powerful and effective tool for testing applications. (Column 2, Lines 28 to 54) It would have been obvious to one having ordinary skill in the art to evaluate line quality as suggested by *Maurer et al.* to change recognition algorithms and recognition parameters as taught by *Su et al.* for the purpose of providing a tool for testing and improving a speaker verification system due to changing background noise conditions.

Response to Arguments

7. Applicant's arguments filed 08 August 2005 have been fully considered but they are not persuasive.

Applicant argues that *Ritter* does not disclose security authorization on both the client and the server that uses biometric data. Applicant states that *Ritter* only discloses use of biometric data for authorization on the client. Applicant maintains that *Ritter*'s authorization on the server is a confirmation of the keys used to perform the client authorization. Also, Applicant says that the biometric keys on the server and the biometric keys on the client are the same, and that one and only one set of biometric data is received by the client. Thus, Applicant's position is that *Ritter* fails to anticipate the independent claims because the same biometric keys are stored on the client and

the server, and only one set of biometric data is obtained to perform the authorization. This is not persuasive.

It is noted that the terms "first and second biometric data" and "first and second level security authorization procedures" are entitled to broad construction. During patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." *In re Hyatt*, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000). Applicant always has the opportunity to amend the claims during prosecution, and broad interpretation by the examiner reduces the possibility that the claim, once issued, will be interpreted more broadly than is justified. *In re Prater*, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969) During examination, the claims must be interpreted as broadly as their terms reasonably allow. *In re American Academy of Science Tech Center*, ___ F.3d___, 2004 WL 1067528 (Fed. Cir. May 13, 2004) Claim terms are presumed to have the ordinary and customary meanings attributed to them by those of ordinary skill in the art. *Sunrace Roots Enter. Co. v. SRAM Corp.*, 336 F.3d 1298, 1302, 67 USPQ2d 1438, 1441 (Fed. Cir. 2003); *Brookhill-Wilk 1, LLC v. Intuitive Surgical, Inc.*, 334 F.3d 1294, 1298 67 USPQ2d 1132, 1136 (Fed. Cir. 2003) See MPEP 2111 and 2111.01. Here, the term "first biometric data" is construed to be information received from a video sensor or microphone from a user of body features, such as eye patterns, facial features, fingerprints, or speech, from which are derived current biometric keys by *Ritter*. (Column 4, lines 15 to 37: Figure 1) The term "second biometric data" is construed to be information on SIM-card 3 of tables 4 of stored biometric keys by *Ritter*. (Column 3,

Line 57 to Column 4, Line 2; Column 4, Lines 35 to 45: Figure 1) The term "first level security authorization procedure" is construed as a comparison on communication terminal device 1 of current biometric data received at a video sensor 2 or microphone from a user to biometric keys stored in SIM-card 3 so as to permit a user authorized usage of a mobile radio telephone 1 by *Ritter*. (Column 4, Lines 16 to 48: Figure 1) The term "second level security authorization procedure" is construed as confirming the authenticity and integrity of the stored biometric keys 4 on personal SIM-card 3 by means of stored tables 11 of biometric keys on biometric server 10 through transmission of stored biometric tables 4 on personal SIM-card 3 to stored biometric tables 11 on biometric server 10 by *Ritter*. (Column 4, Lines 37 to 40: Figure 1)

Clearly, the first and second biometric data and the first and second level security authorization procedures are not the same in *Ritter*, as contended by Applicant. *Ritter*'s first biometric data is a current biometric key derived from a user's body features or voice. *Ritter*'s second biometric data is a table of stored biometric keys on SIM-card 3. Both *Ritter*'s first biometric data and second biometric data are received from a user because a user provides both his fingerprint, voice, etc., and his SIM-card 3 to communication terminal device 1. Moreover, the first and second level security procedures are distinct in *Ritter*. A first level security procedure is performed on communication terminal device 1 by comparing a current biometric key derived from a user's body features or voice with a stored biometric key from a table 4 of biometric keys on SIM-card 3 in *Ritter*. A second level security procedure is performed on biometric server 10 by comparing stored biometric keys transmitted from table 4 on

SIM-card 3 with stored biometric keys from table 11 on biometric server 10 in *Ritter*. Thus, a first level security authorization procedure authorizes a user with respect to a user's SIM-card, and a second level security authorization procedure authorizes a user's SIM-card with respect to possible valid SIM-cards. The second level security procedure provides an additional check by testing for possibly fraudulent SIM-cards 3.

Applicant has misconstrued *Ritter* by contending that the first and second biometric data are the same. It is true that *Ritter* says, "The same information is likewise stored on the personal SIM card 3 of the user. . . ." (Column 3, Lines 57 to 58) However, this merely describes the situation, where, in an ordinary course of non-fraudulent activity, the biometric keys stored on a user's SIM-card 3 should match one of the authorized biometric keys stored on biometric server 10. Corresponding keys would not be the same if the biometric keys stored on a user's SIM-card 3 were fraudulent, as where an unauthorized user attempted to store biometric keys of his/her own body features on a SIM-card 3. This is what *Ritter*'s second level security authorization procedure is designed to detect. Nor should it be said that the information received from a user as body features 6, 7, or 8, is the same as the information received on the SIM-card 3. Corresponding current biometric keys derived from body features would not be the same as stored biometric keys on SIM-card 3 if an unauthorized user were attempted to use a SIM-card 3 of an authorized user. This is what *Ritter*'s first level security authorization procedure is designed to detect.

Therefore, the rejections of claims 1 to 6, 9 to 13, 18 to 19, 21 to 23, 25 to 27, 31, 35 to 36, and 38 to 42 under 35 U.S.C. 102(e) as being anticipated by *Ritter*, of claims

7, 8, 14 to 17, 24, and 32 to 34 under 35 U.S.C. 103(a) as being unpatentable over *Ritter* in view of *Su et al.*, of claims 20 and 37 under 35 U.S.C. 103(a) as being unpatentable over *Ritter* in view of *Gifford*, and of claims 28 to 30 under 35 U.S.C. 103(a) as being unpatentable over *Ritter* in view of *Su et al.* and further in view of *Maurer et al.*, are proper.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Martin Lerner whose telephone number is (571) 272-7608. The examiner can normally be reached on 8:30 AM to 6:00 PM Monday to Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Richemond Dorvil can be reached on (571) 272-7602. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ML
9/13/05

Martin Lerner
Examiner
Group Art Unit 2654